

Express Mail Label: EL532334848US  
Date of Deposit: December 20, 1999  
ASSISTANT COMMISSIONER FOR PATENTS  
BOX PATENT APPLICATION  
Washington, D.C. 20231

CASE DOCKET NO. YO999-558  
Date: December 20, 1999

Sir:

jc377 U.S. PTO



12/20/99

Transmitted herewith for filing is the Patent Application of:

Inventors: Yuriy A. Baransky, Hubertus Franke, Pratap C. Pattnaik,  
David R. Safford and Robert W. Wisniewski

For: A METHOD OF SECURELY SHARING INFORMATION OVER PUBLIC NETWORKS USING  
UNTRUSTED SERVICE PROVIDERS AND TIGHTLY CONTROLLING CLIENT ACCESSIBILITY

Enclosed are:

Express Mail Label: EL532334848US  
December 20, 1999

☒ Six (3) Sheets of informal Drawings.

☒ An assignment of the invention to International Business Machines  
Corporation, Armonk, New York 10504.

☐ Certified copy of UK Patent Application No.

☒ Declaration and Power of Attorney is attached to the application.

☐ Associate Power of Attorney.

☐ Information Disclosure Statement with form PTO-1449 with references  
attached.

The filing fee has been calculated as shown below:

	(Col. 1)	(Col. 2)
FOR:	NO. FILED	NO. EXTRA
BASIC FEE		
TOTAL CLAIMS	17- 20 =	0
INDEP CLAIMS	9- 3 =	6
____ MULTIPLE DEPENDENT CLAIM PRESENTED		

If the difference in Col. 1 is less than  
zero, enter "0" in Col. 2.

OTHER THAN A  
SMALL ENTITY

RATE	FEE
	\$ 760.00
X \$ 18 =	\$
X \$ 78 =	\$ 468.00
+ \$ 260 =	\$
TOTAL	\$ 1228.00

☒ Please charge my Deposit Account No. 09-0468 in the amount  
of \$1228.00.

☒ The Commissioner is hereby authorized to charge payment of the  
following fees associated with this communication or credit any  
overpayment to Deposit Account No. 09-0468. A duplicate copy of  
this sheet is enclosed.

☒ Any additional filing fees required under 37 CFR 1.16.

☒ Any patent application processing fees under 35 CFR 1.17.

Respectfully submitted,

By

Attorney: Douglas W. Cameron  
Registration No.: 31,596  
Tel. (914) 945-3244

IBM CORPORATION  
INTELLECTUAL PROPERTY LAW DEPT.  
P.O. BOX 218  
YORKTOWN HEIGHTS, NY 10598

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Yuriy A. Baransky et al.

Serial No.: Unassigned

Group No. Unassigned

Filed: Herewith

Examiner: Unassigned

For: A METHOD OF SECURELY SHARING INFORMATION OVER  
PUBLIC NETWORKS USING UNTRUSTED SERVICE PROVIDERS  
AND TIGHTLY CONTROLLING CLIENT ACCESSIBILITY

Commissioner of Patents and Trademarks  
Washington, D.C. 20231

EXPRESS MAIL CERTIFICATE

Express Mail Label Number EL532334848US

Date of Deposit December 20, 1999

I hereby certify that the attached paper or fee

Patent Application Transmittal Letter (original and one copy)

Patent Application

3 Figures

Assignment

Assignment Cover Sheet

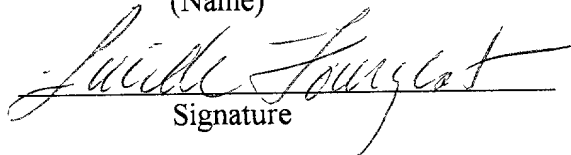
Declaration and Power of Attorney

Self Addressed Return Postcard

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Lucille Fourgeot

(Name)

  
Signature

**Note:** Each paper must have its own certificate and the "Express Mail" label number as a part thereof or attached thereto. When, as here, the certification is presented on a separate sheet, that sheet must (1) be signed and (2) fully identify and be securely attached to the paper or fee it accompanies. Identification should include the serial number and filing date of the application as well as the type of paper being filed, e.g. complete application, specification and drawings, responses to rejection or refusal, notice of appeal, etc. If the serial number of the application is not known, the identification should include at least the name of the inventor(s) and the title of the invention.

**Note:** The label number need not be placed on each page. It should, however, be placed on the first page of each separate document, such as, a new application, amendment, assignment, and transmittal letter for a fee, along with the certificate of mailing by "Express Mail". Although the label number may be on checks, such a practice is not required. In order not to deface formal drawings it is suggested that the label number be placed on the back of each formal drawing or the drawings be accompanied by a set of informal drawings on which the label number is placed.

Docket No. YO999-558

# A Method of Securely Sharing Information Over Public Networks Using Untrusted Service Providers and Tightly Controlling Client Accessibility.

## Description

### Technical Field

This invention relates to the field of securely sharing information over a public network.

### Background of the Invention

The internet has emerged as a fundamental medium of public communication. Nevertheless, restricting access from the general public to a selected subset is useful as evidenced by the growing use of firewalls and encryption technologies. There are also different schemes such as the Secure Sockets Layer (SSL) that provide for restricted access to a set of web pages.

However, these techniques depend critically on the service provider to ensure that access policies are enforced based on IP addresses (firewalls) or passwords and keys (encryption, SSL). While for large companies this may be a suitable technique, for individuals or for small companies using a service provider this technique is questionable because they must place trust in a third party. All methods, including those trusting the service providers, allow a proliferation of accessibility once one client can enter the protected area. For example, a scheme with a userid and password can easily be, and is frequently, distributed along insecure channels (e.g., verbal communication, e-mail, or worse posting on the net), thus preventing the provider from maintaining control over who has access to the content.

Data encryption systems are well known in the data processing art. In general, such systems operate by performing an encryption operation on a plaintext input block, using an encryption key, to produce a ciphertext output block. The receiver of an encrypted message performs a corresponding decryption operation, using a decryption key, to recover the original plaintext

block. The goal of encryption is confidentiality, that is to prevent anyone other than holders of the key from reading the data.

Encryption systems fall into two general categories. Symmetric (or secret key) encryption systems such as the Data Encryption Standard (DES) system use the same secret key for both encrypting and decrypting messages. In the DES system, a key having 56 independently specifiable bits is used to convert 64-bit plaintext blocks to ciphertext blocks, or vice versa. Asymmetric (or public key) encryption systems, on the other hand, use different keys that are not feasibly derivable from one another for encryption and decryption. A person wishing to receive messages generates a pair of corresponding encryption and decryption keys. The encryption key is made public, while the corresponding decryption key is kept secret. Anyone wishing to communicate with the receiver may encrypt a message using the receiver's public key. Only the receiver may decrypt the message, however, since only he has the private key.

In addition to confidentiality, two other goals of cryptographic systems are authentication and integrity. Authentication is concerned with verifying the identity of the sender of the received data, and integrity is concerned with verifying that the data has not been modified. Authentication and integrity of data are often combined in a Message Authentication Code (MAC), which cryptographically verifies both properties.

Secure Sockets Layer (SSL) is a cryptographic protocol for use in web communication, which is designed to provide authenticity, integrity, and confidentiality. This protocol is integrated into many web server and client software packages, but the web server must be configured by the service provider to use SSL, and the content owners are typically unable to control its use.

As the desire of individuals to produce personal pages to be shared with a selected set of geographically dispersed clients (e.g. family members) grows, and as the number of small businesses (those without internal ISP support, i.e., those that rely on service providers) who sell products over the web grows, there arises an increased need to provide security. Specifically, the security model desired by these groups of content providers is one with which they can personally

guarantee, without having to trust their service provider, and a model with which they can maintain tight control on which clients have access to their content.

### Summary of the Invention

5 This invention provides a method for allowing a content provider to restrict access to a collection of web pages or information without the involvement of a service provider. Access is controlled with a one-time handshaking protocol established between the content provider and a client or user using a specific machine. Through a secure exchange of information during this handshaking protocol, a client using a specific machine is uniquely identified for the purposes of accessing the information or web pages subsequent to the completion of the handshaking protocol. The same  
10 user or client can not access the information from another machine. Thus, with this invention, a virtual private network is established that gives protected content information only to authorized users using specific machines. Since the protected content is encrypted when it is transmitted to the specific machine the service provider does not have access to the content at transmittal point. Further, even though the data is stored on the content provider's disk, it is stored in an encrypted form with only the content provider knowing the decryption key. Thus, both during storage and  
15 transmittal, the data is encrypted and neither the service provider nor an unintended third party has access to the data.

Thus, it is an object of this invention to pass information from a content provider to a specific user on a specific machine without having to trust a service provider.

20 It is another more specific object of this invention to control access to content by restricting the number of different machines from which a user may access the protected content.

It is also a more specific object of this invention to prevent the practice of a client giving out his or her user ID and password to allow any other user to access the protected content from any machine.

It is also an object of this invention to provide for the protection of content without the need for creation and maintenance of public/private keys.

Preventing proliferation of access is accomplished by doling out one-time keys that are used to establish a mapping between the client machine and the content provider. The one-time key includes a unique number generated by the content provider. Upon receiving an initialization request, the content provider queries the client machine for a unique piece of information identifying the machine. That information is securely transmitted back to the content provider and an encrypted, opaque cookie is stored on the client's machine for future accesses. After initialization, when the client attempts access to the content provider's web page, both the cookie and the unique piece of information tied to this machine are required to gain access. An applet is downloaded upon discovering a special encrypted web page, and the applet finds a cookie associated with a tag provided by the content provider. The applet looks up the required part of the unique piece of information identifying the machine, sends it to the content provider, and access to the page is granted after the information is verified. As an extra measure of security, for local control, or for use in a shared environment, a userid/password pair can be asked for at this point.

### **Brief Description of the Drawings**

FIG. 1. Illustrates initialization phase, which is the series of actions that need to occur the first time a new user accesses the web page.

FIG. 2. Illustrates the access phase, which is the series of actions that occur each time a known user access the web page.

FIG. 3 is a table maintained by the content provider showing the mapping between the userid-id and machine-id, the one-time password, and the session key.

### **Description of the Preferred Embodiment**

From a client's perspective accessing an encrypted web page as provided by this invention appears identical to the access of any other web page. The only difference is that the first time the client accesses the web page, a userid and a one-time password will be required. Thereafter, the

software on the client's machine will coordinate with the security software of the server's machine to seamlessly provide the web pages as if the encryption did not exist.

### Notations Used In This Application

**IDu** - unique identification of user

5 **IDm** - unique identification of machine

**PWu** - a one time user password

**Ka** - a symmetric encrypting key

**Na** - random nonce

**a\*b** - a multiplied by b

10 **Ka(b)** - data b is encrypted with symmetric key Ka

**g** - preselected common base

**g<sup>a</sup>** - g to the power a

**ab** - concatenate \*(put together) "a" and b

**MAC** - Message Authenticated Code

15 A MAC is a keyed hash that strongly authenticates a message. If any bit is changed or incorrect in the hash sequence it is detectable and interpreted as being the incorrect code.

**MAC(a, bc)** - perform a MAC with a and with the key which is b concatenated with c.

20 The following definitions are used throughout this embodiment:

**Content Provider** - a user that makes a web page or other information available for access by other users on the net. The content provider is also referred to as the server because it is the content provider that is providing or serving the web pages.

**Service Provider** - a company that provides disk space and internet access.

Client - also referred to as user - a user that is interested in viewing information provided by the Content Provider

For a user or client to obtain the capability of accessing an encrypted web page provided by a server (content provider), a userid IDu needs to be assigned to the client, and a one-time password PWu needs to be given to the user. The transport of the IDu and one-time password PWu can be by any means, e.g. e-mail, US mail, phone, etc. Once this transport occurs and prior to standard access of the encrypted web page, a one-time initialization phase needs to occur (See FIG. 1). The purpose of this initialization phase is to create a one-to-one mapping between the client and the identity of the machine (IDm) the client is using. This phase is mostly hidden from the client except that at first access the client will be asked to provide the userid (IDu) and a one-time password (PWu) that were provided to the client as indicated above. The request for IDu and PWu will be generated by an applet that is downloaded to the client's machine from the server's machine upon access to the encrypted web page. Once IDu and PWu are provided by the client, the establishment phase occurs automatically, and all future references to the web page occur without prompting the client for IDu and PWu. Note, that content providers, such as companies selling information via web pages, are not precluded from continuing to require a userid and password upon each new entrance to their site. With this invention, clients can no longer give out their userid and password to other clients because there is also a machine-id (IDm).

As mentioned, the first time a client accesses an encrypted web page, an initialization phase needs to occur. This phase establishes the one-to-one mapping between the client and client's machine as kept track of in FIG. 3. This phase is visible to the user only in that the user is prompted for a userid and one-time password. Conceptually, what occurs during this phase is that the server (content provider) executes a protocol to establish a unique relationship with a client and machine pair. By default, for IDm, the invention uses a varying subset of the unique hardware network identifying address. This identifier can be the unique identifier on the network card on every machine, or other unique identifier e.g., pentium III cpu-id. The invention can be augmented to take advantage of a smart card. A smart card is hardware plugged into the client machine that



generates unique and varying keys in a way that guarantees the machine is what it claims to be and as such provides much stronger guarantees.

Upon any incoming request for the web page, an applet is downloaded to the client's machine to identify the accessing computer. This applet contains  $K_c$  and thus can decrypt the encrypted  $K_c(K_a b)$  key stored on the client machine. As the applet is loaded, a varying set of bits from  $ID_m$  is requested. The initialization phase as shown in FIG. 1 is initiated if the applet returns bits from an unknown  $ID_m$  to the content provider's machine. When the server finds that it is not aware of the requesting client's machine, it has the applet execute the first step (11) in FIG. 1. As part of this first step, the applet obtains the whole unique machine identifier ( $ID_m$ ), prompts the user for his or her userid ( $ID_u$ ), calculates  $G^a$  (where  $G$  and  $a$  are random numbers) and transmits these three items back to the server. In step 12 of FIG. 1, the server generates random numbers  $b$  and  $N_b$ , generates  $G^b$  and  $G^{(a*b)} = K_a b$ , encrypts  $G^b$  with the one-time password  $PW_u$ , and encrypts  $N_b$  with  $K_a b$ . The results of step 12 are transmitted to the client machine. When the client machine receives these results, the user is prompted for the one-time password, which can be used to decrypt the encrypted  $G^b$ , where  $G^b$  is used to calculate  $K_a b$ , which in turn is used to determine  $N_b$ . If the client fails to correctly provide  $PW_u$  then the algorithm with failure; no cookie gets stored on the client machine with the result being this client has not gained access to the content provider's data. If the correct  $PW_u$  is provided, the applet generates a random number  $N_a$ , encrypts  $N_a$  with the session key  $K_a b$ , and performs a Message Authenticated Code (MAC) on  $K_a b$  and  $N_a N_b$ . See step 13 in FIG. 1. The applet then sends the results as shown in step 13 to the server. The server verifies the MAC operation, stores the session key  $K_a b$  and the userid-machine ID pair, and sends MAC ( $K_a b$ ,  $N_a N_b$ ) to the client machine. See step 14 in FIG. 1. The client then verifies the MAC to make sure that the previous message in 14 actually came from the server. The client machine then stores an encrypted version of the session key ( $K_c$ ) ( $K_a b$ ), where the encrypted version of the session key will be used to subsequently access the web page. As an additional measure of security, recommended on multi-user systems, the user can be prompted for a separate password (different from  $PW_u$ ). This password is used to encrypt the  $K_c(K_a b)$  so only this user of the system can gain access. At this point, the initialization phase is now complete. The server has securely created a mapping between the userid ( $ID_u$ ) and the

machine (IDm), and the server has stored the IDu and the IDm for future allowing the client to subsequently access the web page. The server also has stored the session key Kab which will be used to securely communicate with the client. See Fig. 3 for the data structure used to store the above mentioned information. The protocol immediately moves to the access phase. Future references also proceed to the access phase since once the applet is downloaded it will recognize that the client's browser has a cookie associated with this content provider's page.

Note: The password PWu is considered one time because it is never used again. It is used only during the initialization phase to establish the user:machine mapping. Observe that a potential security problem exists if someone steals and uses the userid and password before the intended client is able to use them. The security exposure is therefore limited to the time frame of sending out a one-time password until its usage at initial access. The access can easily be retracted in the event the intended individual was not the client that made use of the one-time password. Thus, a follow up with the expected client would be prudent. However, as soon as the client notifies the content provider that they have not accessed the page, even though the server thinks they have, the userid can be revoked and the process redone. The power of the one-time password linked to establishing the unique user:machine mapping is that it prevents the proliferation of accessibility to the server, i.e., once the client uses the password it is never again useful for friend or foe. Note that this also prevents the client from being able to access the web page from multiple machines or access points. This problem is easily remedied by just providing two one-time passwords to such a user. What the invention does allow, however, is for the content provider to obtain very strict control over how widespread the ability to access this page or information is.

Referring to FIG. 2, the first step of the access phase begins with the applet picking a random  $x$  and sending a scrambled and varying subset of the machine IDm. This applet, as in the previous discussion, is downloaded to the client's machine (and contains Kc) when the client accesses the content provider's data. The applet also sends the userid and  $g^x$ . See 21 of FIG. 2. The server verifies that the subset of bits from the machine id IDm matches what it expected from the user id. If there is a match, the content provider generates a random  $y$  and sends  $g^y$ , else it just sends an authentication failure message to the user. (22 in FIG. 2). Upon receiving  $g^y$ , i.e., success, the

applet performs a MAC with key  $K_{ab}$ , and sends  $MAC(K_{ab}, M2M1)$  to the server, where  $M1 = (ID_u, ID'_m, g^x)$  and where  $M2 = g^y$ , where  $x$  is a random number generated by the client machine, and where  $y$  is a random number generated by the content provider. This is accomplished because the applet knows  $K_c$  and can thus decrypt  $K_c(K_{ab})$ . If there was an additional optional separate user-provided password (as described in the above embodiment) then the user will be prompted for that. The client's response proves that it has seen  $M1$  and  $M2$  and knows  $K_{ab}$ . (23 in FIG. 2). The server verifies the MAC, and sends  $MAC(K_{ab}, M1M2)$  back to the client. This last step proves to the client that the server is who it is claiming to be and nobody else is masquerading as the server (24 in FIG. 2). The Content Provider decrypts the page with its own encryption key, and re-encrypts it with the new session key ( $K_{xy}$ ). Since the content is encrypted when it is transmitted to the specific machine the service provider does not have access to the content at the transmittal point. Further, even though the data is stored on the content provider's disk, it is stored in an encrypted form with only the content provider knowing the decryption key. Thus, both during storage and transmittal, the data is encrypted and neither the service provider nor an unintended third party has access to the data. Once the data is re-encrypted and securely delivered to the client, the applet can now use the new session key to decrypt the page and display the content for the user (26 in FIG. 2).

### Claims

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

1. A method for securely providing data of a content provider to a user without trusting an internet service provider, said method comprising:
  - a. generating a first key known only to said content provider;
  - b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password;
  - c. storing said encrypted second key on a client machine; and
  - d. decrypting said second encrypted key using said first key; and
  - e. accessing said data using said second key.
2. A method as recited in claim 1, further comprising the step of transmitting the identity of said client machine to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only on said client machine.
3. A method as recited in claim 1, wherein said one-time password is a unique user identifier and wherein said one-time password is transmitted out of band.
4. A method as recited in claim 1, wherein said second key is required in an algorithm that generates a session key which is used to decrypt said data.
5. A method for securely providing data of a content provider to a user without trusting an internet service provider, said method comprising:
  - a. generating a first key known only to said content provider;
  - b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password and a separate user provided password;
  - c. storing said encrypted second key on a client machine; and
  - d. decrypting said second encrypted key using said user provided password; and

e. accessing said data using said second key.

6. A method as recited in claim 5, further comprising the step of transmitting the identity of said client machine to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only on said client machine.

5 7. A method as recited in claim 5, wherein said one-time password is a unique user identifier and wherein said one-time password is transmitted out of band.

8. A method as recited in claim 5, wherein said second key is required in an algorithm that generates a session key which is used to decrypt said data.

10 9. In a communications network having at least a content provider node and a plurality of client machines, a method of authenticating a user seeking access to secure data of said content provider, said method comprising:

a. transmitting  $g^a$  and the identity of the user of said one client machine to said content provider node, where  $g$  and  $a$  are random numbers and where  $a$  is known only to said client machine, and where  $g$  is known to both content provider node and said client machine;

15 b. generating  $g^b$ , where  $b$  is known only to said content provider node;

c. encrypting  $g^b$  with a one-time password of said user;

d. calculating  $g^{(a*b)}$  by said client machine using said one-time password to decrypt said encrypted  $g^b$ ; and

20 e. transmitting  $g^{(a*b)}$  to said content provider, whereby said client machine's knowledge of  $g^{(a*b)}$  authenticates said user to said content provider.

10. A method as recited in claim 9, further comprising the step of transmitting the identity of a particular one of said client machines to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only by said user on said client machine.

25 11. A method as recited in claim 9, further comprising the step of performing a method authenticated code on  $g^{(a*b)}$  at said content provider and transmitting results of performing said method authenticated code to said client, where said client machine verifies said results to authenticate said content provider.

12. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for securely providing data of a content provider to a user, said method comprising:

- a. generating a first key known only to said content provider;
- 5 b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password;
- c. storing said encrypted second key on a client machine; and  
when said user desires to access said data:
- d. decrypting said second encrypted key using said first key; and
- 10 e. accessing said data using said second key.

13. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for securely providing data of a content provider to a user, said method comprising:

- a. generating a first key known only to said content provider;
- 15 b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password and a separate user provided password;
- c. storing said encrypted second key on a client machine;  
when said user desires to access said data:
- d. decrypting said second encrypted key using said user provided password; and
- 20 e. accessing said data using said second key.

14. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for use in a communications network having at least a content provider node and a plurality of client machines, said method steps authenticating a user seeking access to secure data of said content provider, said method steps comprising:

- a. transmitting  $g^a$  and the identity of the user of said one client machine to said content provider node, where  $g$  and  $a$  are random numbers and where  $a$  is known only to said client machine, and where  $g$  is known to both content provider node and said client machine;
- b. generating  $g^b$ , where  $b$  is known only to said content provider node;

- c. encrypting  $g^b$  with a one-time password of said user;
- d. calculating  $g^{(a*b)}$  by said client machine using said one-time password to decrypt said encrypted  $g^b$ ; and
- e. transmitting  $g^{(a*b)}$  to said content provider, whereby said client machine's knowledge of  $g^{(a*b)}$  authenticates said user to said content provider.

15. A computer program product for securely providing data of a content provider to a user without trusting an internet service provider, said computer program product comprising:

- a. first instruction means for generating a first key known only to said content provider;
- b. second instruction means for encrypting a second key using said first key and an encryption algorithm requiring a one-time password;
- c. third instruction means for storing said encrypted second key on a client machine; and when said user desires to access said data;
- d. fourth instruction means for decrypting said second encrypted key using said first key; and
- e. accessing said data using said second key.

16. A computer program product for securely providing data of a content provider to a user without trusting an internet service provider, said computer program product comprising:

- a. first instruction means for generating a first key known only to said content provider;
- b. second instruction means for encrypting a second key using said first key and an encryption algorithm requiring a one-time password and a separate user provided password;
- c. third instruction means for storing said encrypted second key on a client machine; and when said user desires to access said data;
- d. fourth instruction means for decrypting said second encrypted key using said user provided password; and
- e. fifth instruction means for accessing said data using said second key.

17. A computer program product for use in a communications network having at least a content provider node and a plurality of client machines, said computer program for authenticating a user seeking access to secure data of said content provider, said computer program product comprising:

- a. transmitting  $g^a$  and the identity of the user of said one client machine to said content provider node, where  $g$  and  $a$  are random numbers and where  $a$  is known only to said client machine, and where  $g$  is known to both content provider node and said client machine;
- b. generating  $g^b$ , where  $b$  is known only to said content provider node;
- 5 c. encrypting  $g^b$  with a one-time password of said user;
- d. calculating  $g^{(a*b)}$  by said client machine using said one-time password to decrypt said encrypted  $g^b$ ; and
- e. transmitting  $g^{(a*b)}$  to said content provider, whereby said client machine's knowledge of  $g^{(a*b)}$  authenticates said user to said content provider.



## Method of Securely Sharing Information Over Public Networks Using Untrusted Service Providers and Tightly Controlling Client Accessibility

### Abstract

- 5 A method for allowing a content provider to restrict access to data without having to trust a service provider. With this invention a content provider is able to restrict access to data to a specific client using a specific machine. A content provider generates a first key which is used to encrypt a second key where the second key will only be encrypted if the user has a one-time password. The encrypted second key is then stored on the client machine. When the user desires to access the data of the content provider, the second key is decrypted and used to access the data.

## Initailization Phase (one time)

Client

Content Provider

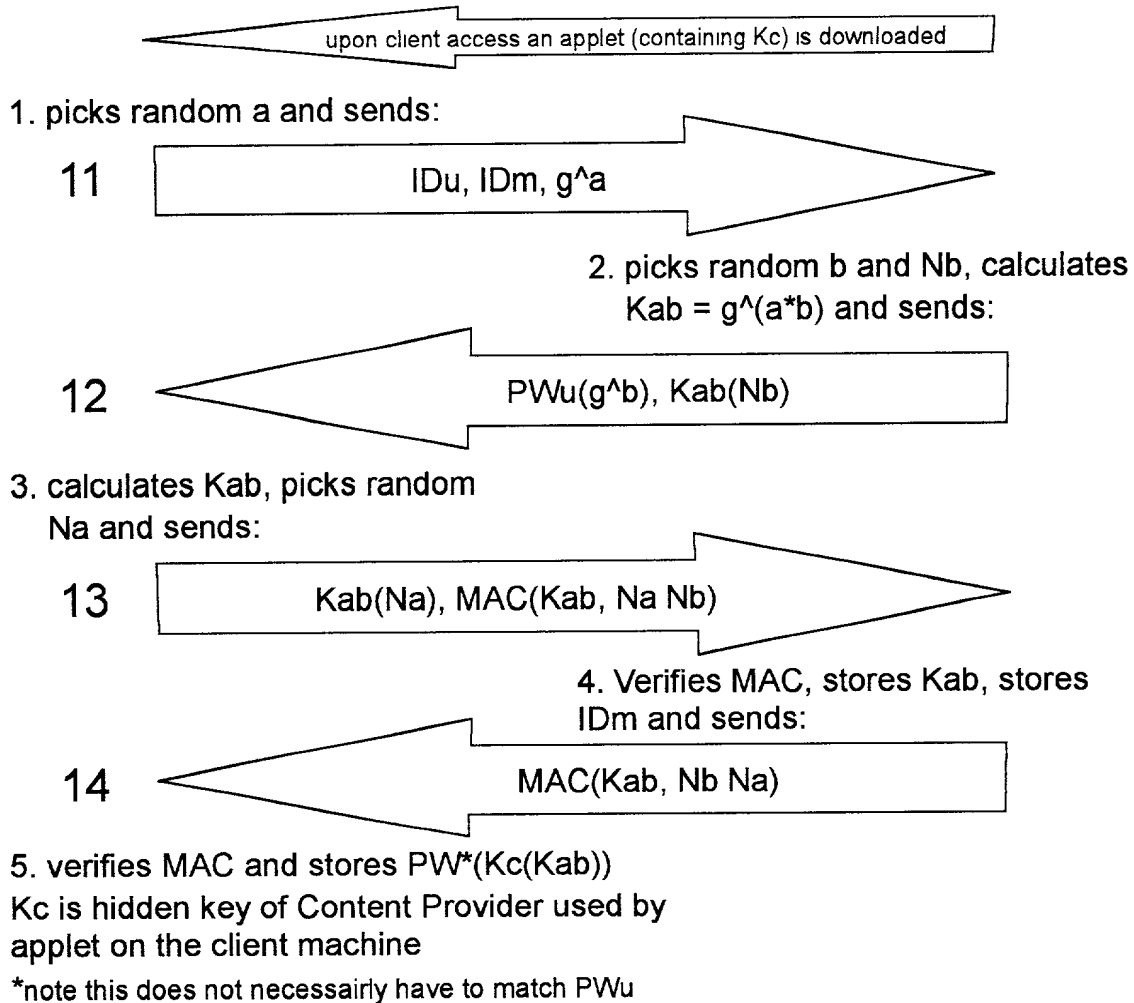


Fig. 1

## Access Phase

Client

Content Provider

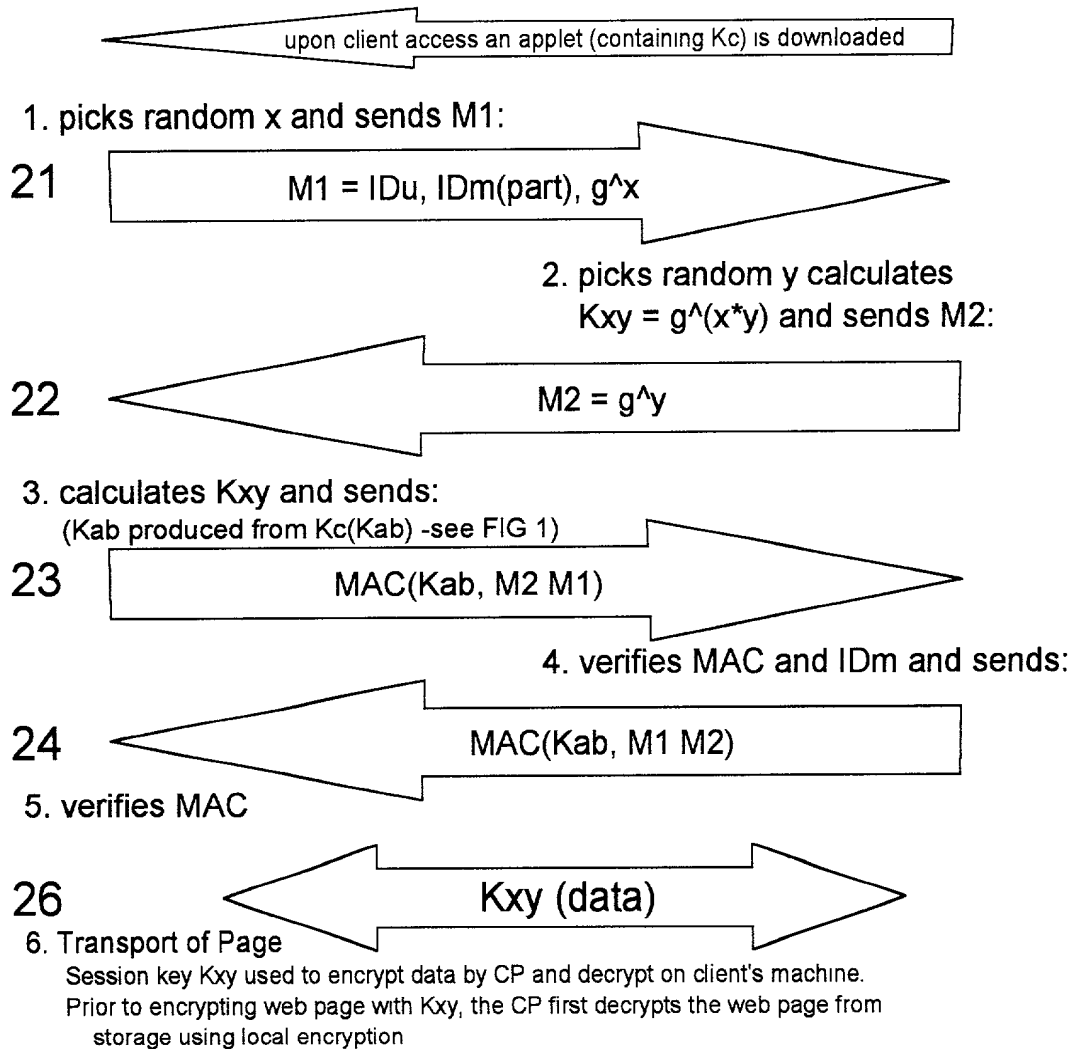


Fig. 2

## Table of Information kept by Content Provider

Users	IDm	IDu	PWu	Kab
User1				
User2				
User3				
User4				

Fig. 3

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**A METHOD OF SECURELY SHARING INFORMATION OVER PUBLIC NETWORKS USING UNTRUSTED SERVICE PROVIDERS AND TIGHTLY CONTROLLING CLIENT ACCESSIBILITY**

the specification of which (check one)

☒ is attached hereto. or PCT International Application Number \_\_\_\_\_

\_\_\_\_\_ was filed on \_\_\_\_\_ as United States Application Number \_\_\_\_\_

and was amended on \_\_\_\_\_ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application, which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

_____ (Application Number)	_____ (Filing Date)
_____ (Application Number)	_____ (Filing Date)

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)
_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)


I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number).

Manny W. Schecter (Reg. 31,722), Terry J. Ilardi (Reg. 29,936), Christopher A. Hughes (Reg. 26,914), Edward A. Pennington (Reg. 32,588), John E. Hoel (Reg. 26,279), Joseph C. Redmond, Jr. (Reg. 18,753), Douglas W. Cameron (Reg. 31,596), Louis P. Herzberg (Reg. 41,500), Wayne L. Ellenbogen (Reg. 43,602), Stephen C. Kaufman (Reg. 29,551), Daniel P. Morris (Reg. 32,053), Paul J. Otterstedt (Reg. 37,411), Louis J. Percello (Reg. 33,206), Jay P. Sbröllini (Reg. 36,266), David M. Shofi (Reg. 39,835) and Robert M. Trepp (Reg. 25,933)

Send Correspondence to: Douglas W. Cameron, Intellectual Property Law Dept.IBM Corporation, P.O. Box 218, Yorktown Heights, New York 10598Direct Telephone Calls to: (name and telephone number) Douglas W. Cameron (914) 945-3244Yuri J Andri J Baransky

Full name of sole or first inventor

Inventor's Signature Date 12-16-199963 Kings Ferry Road, Montrose, New York 10548  
ResidenceUSA  
CitizenshipSame as above.  
Post Office Address

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATIONHubertus Franke

Full name of second joint-inventor, if any

Hubertus Franke

Inventor's signature

12-1-99

Date

27 Greenlawn Road, Cortlandt Manor, New York 10567  
ResidenceGermany  
CitizenshipSame as above.  
Post Office AddressPratap Chandra Pattnaik

Full name of third joint-inventor, if any

Pratap Chandra Pattnaik

Inventor's signature

12-1-99

Date

213 Barnes Street, Ossining, New York 10562  
ResidenceUSA  
CitizenshipSame as above.  
Post Office AddressDavid R. Safford

Full name of fourth joint-inventor, if any

David R Safford

Inventor's Signature

12/1/99

Date

16 Indian Hill Road, Brewster, New York 10509  
ResidenceUSA  
CitizenshipSame as above.  
Post Office AddressRobert William Wisniewski

Full name of fifth joint inventor, if any

Robert William Wisniewski

Inventor's Signature

11-29-99

Date

253 Maple Brook Court, Yorktown Heights, New York 10598  
ResidenceUSA  
CitizenshipSame as above.  
Post Office Address

Full name of sixth joint-inventor, if any

Inventor's signature

Date

Residence

Citizenship

Post Office Address